PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-081969
(43)Date of publication of application : 21.03.2000

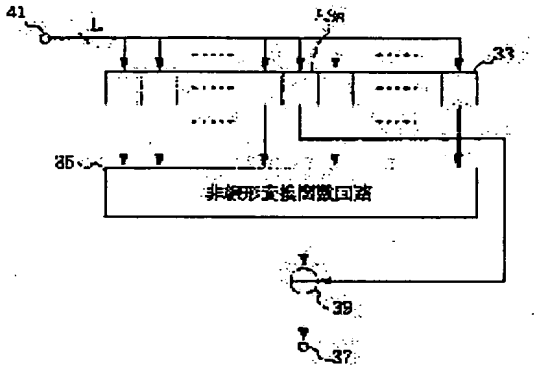
(51)Int.Cl. G06F 7/58

(21)Application number : 10-267415
(22)Date of filing : 04.09.1998

(71)Applicant : KUROSAWA KAORU
TOYO COMMUN EQUIP CO LTD
(72)Inventor : KUROSAWA KAORU
SUGIMOTO KOICHI

(54) PSEUDO-RANDOM NUMBER GENERATOR

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain good random number characteristics by assuring equal frequency characteristics of output by performing an exclusive OR operation between at least one register value of a linear feedback shift register and a nonlinear transformation value of the remaining register values.
SOLUTION: A nonlinear transformation function circuit 35 is connected with the linear feedback shift register 33 with L stages to generate an (m) system. In addition, an exclusive OR operation circuit 39 is connected between the nonlinear transformation function circuit 35 and an output terminal 37. Output of at least one stage 33a of the linear feedback shift register 33 with L stages is connected with the other input of the exclusive OR operation circuit 39. Since the linear feedback shift register 33 has a cycle of 2L-1, when L is sufficiently large, kinds of appearance probability of 1, 0 of output in a nonlinear filter generator with this structure are regarded as equal. Therefore, the pseudo-random number generator with good random number characteristics in which kinds of appearance of 1, 0 are in equal frequency is obtained.



LEGAL STATUS

[Date of request for examination]	27.09.2000
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3533956
[Date of registration]	19.03.2004
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－81969
（P2000－81969A）
(43)公開日　平成12年３月21日(2000.3.21)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'（参考）
Ｇ０６Ｆ　7/58		Ｇ０６Ｆ　7/58	Ｃ

審査請求　未請求　請求項の数２　ＦＤ　（全 8 頁）

(21)出願番号　特願平10－267415

(22)出願日　平成10年９月４日(1998.9.4)

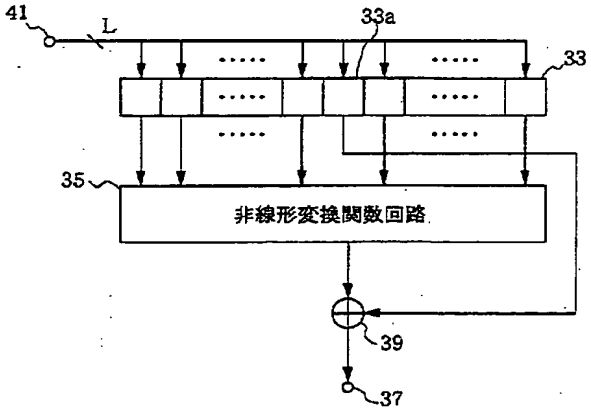
特許法第30条第１項適用申請有り　1998年３月６日　社団法人電子情報通信学会発行の「1998年電子情報通信学会総合大会講演論文集基礎・境界」に発表

(71)出願人　598129163
黒澤　馨
神奈川県川崎市高津区諏訪２－７－３　パステルハイツ205
(71)出願人　000003104
東洋通信機株式会社
神奈川県高座郡寒川町小谷２丁目１番１号
(72)発明者　黒澤　馨
神奈川県川崎市高津区諏訪２－７－３　パステルハイツ205
(74)代理人　100085660
弁理士　鈴木　均

最終頁に続く

(54)【発明の名称】　擬似乱数発生装置

(57)【要約】
【課題】　出力の１、０の等頻度性を保障して良好な乱数特性を得ることができる擬似乱数発生装置を提供する。
【解決手段】　暗号通信装置などで使用される擬似乱数を発生させる擬似乱数発生装置であって、クロックに同期して動作するｍ系列を生成する線形フィードバックシフトレジスタと、上記線形フィードバックシフトレジスタの各レジスタ値を非線形変換して１ビットの出力を得る非線形変換関数手段と、上記線形フィードバックシフトレジスタに初期値を設定する初期値設定手段と、上記線形フィードバックシフトレジスタ内少なくとも１つの線形フィードバックシフトレジスタのレジスタ値を残りの線形フィードバックシフトレジスタのレジスタ値の非線形変換値と排他的論理和演算を施して擬似乱数として出力する排他的論理和演算手段とを具備する構成となっている。



1

【特許請求の範囲】

【請求項１】　暗号通信装置などで使用される擬似乱数を発生させる擬似乱数発生装置であって、

クロックに同期して動作するｍ系列を生成する線形フィードバックシフトレジスタと、

上記線形フィードバックシフトレジスタの各レジスタ値を非線形変換して１ビットの出力を得る非線形変換関数手段と、

上記線形フィードバックシフトレジスタに初期値を設定する初期値設定手段と、

上記線形フィードバックシフトレジスタ内少なくとも１つの線形フィードバックシフトレジスタのレジスタ値を残りの線形フィードバックシフトレジスタのレジスタ値の非線形変換値と排他的論理和演算を施して擬似乱数として出力する排他的論理和演算手段とを具備することを特徴とする擬似乱数発生装置。

【請求項２】　暗号通信装置などで使用される擬似乱数を発生させる擬似乱数発生装置であって、クロックに同期して動作するｍ系列を生成する線形フィードバックシフトレジスタと、上記線形フィードバックシフトレジスタの各レジスタ値を線形変換し出力する線形変換手段と、上記線形変換値を非線形変換して１ビットを出力する非線形変換手段と、上記線形フィードバックシフトレジスタに初期値を設定する初期値設定手段とを具備し、上記非線形変換手段は、上記線形変換手段の少なくとも１ビットの出力を残りの線形変換手段の非線形変換値と排他的論理和演算を行い擬似乱数として出力するものであって、上記線形変換手段は、線形フィードバックシフトレジスタの状態遷移行列のべきで表現できることを特徴とする擬似乱数発生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号通信装置などで使用される擬似乱数を発生させる擬似乱数発生装置に関し、特に、出力の１、０の等頻度性を保障して良好な乱数特性を得ることができる擬似乱数発生装置としてのフィルタジェネレータに関する。

【０００２】

【従来の技術】従来より、電話、無線、データ通信などの通信システムにおいて、伝送情報が第三者に知られないようにするために、伝送情報を暗号化することが行われる。この暗号化方式で特に高速通信に利用されるものの中にストリーム暗号方式がある。ストリーム暗号方式は、擬似乱数発生装置の出力する擬似乱数を１ビット単位でデータストリームと排他的論理和演算を施すことでデータストリームの暗号化を行うものである。すなわち、一般のストリーム暗号装置は、図４に示す様に、データストリームの入力端子１と出力端子３との間に排他的論理和演算回路５が接続され、上記排他的論理和演算回路５の他方の入力に擬似乱数発生装置７の出力が接続

2

されている。そして、上記擬似乱数発生装置７には入力端子９およびクロック入力端子１１が接続され、初期値およびクロック信号が入力される。図５は従来の擬似乱数発生装置の一例であるノンリニアフィルタジェネレータ（Ｎｏｎｌｉｎｅａｒ　Ｆｉｌｔｅｒ　Ｇｅｎｅｒａｔｏｒ）の構成図を示すものである。図５に示す様に、このノンリニアフィルタジェネレータは、入力端子１３およびクロック入力端子１５に接続された線形フィードバックシフトレジスタ１７に非線形変換関数回路１９が接続され、上記非線形変換関数回路１９に出力端子２１が接続されている。上記ノンリニアフィルタジェネレータは、クロック入力端子１５よりのクロックに同期して動作する線形フィードバックシフトレジスタ１７の各レジスタ値を入力とする非線形変換関数回路１９の出力系列を擬似乱数系列としている。

【０００３】図６に上記線形フィードバックシフトレジスタの一つであるスタンダード型線形フィードバックシフトレジスタの構成を示す。このスタンダード型線形フィードバックレジスタは、図６に示す様に、複数（この場合Ｌ）のレジスタ２３と複数（この場合Ｌ－１）の排他的論理和演算回路２５とが直列に接続され、上記各レジスタ２３の出力と各排他的論理和演算回路２５の一方の入力との間にフィードバックタップ２７が接続されている。上記線形フィードバックシフトレジスタの段数をＬとすると、１つのレジスタに注目した時、出力系列の最大周期は2^L-1となることが知られており、この系列をｍ系列と呼ぶ。例えば、図６に示す線形フィードバックシフトレジスタにおいてｍ系列を生成するには、次のようにする。図６において、$c_1, c_2, \cdots, c_{L-1}$はフィードバックタップと呼ばれ、タップが１のとき結線を示し、０のとき断線を示すものである。このとき線形フィードバックシフトレジスタの出力系列の特性多項式は、次のように表される。

【０００４】

【数１】

$$C(X)=X^L+c_{L-1}X^{L-1}+\cdots+c_1X+1 \quad \cdots(1)$$

上式が原始的な既約多項式となるようにすれば、線形フィードバックシフトレジスタはｍ系列を生成するようになる。図６に示す線形フィードバックシフトレジスタの

時刻t における状態を、

【０００５】

【数２】

$$s(t) = \left(s_L(t), \cdots, s_1(t)\right)^T$$

と表すとき（ここで、Ｔは転置を示す）、１クロック入力後の線形フィードバックシフトレジスタの状態を、

＊【０００６】

【数３】

$$s(t+1) = \left(s_L(t+1), \cdots, s_1(t+1)\right)^T$$

と表せば、状態遷移は、

【０００７】

【数４】

$$\begin{pmatrix} s_L(t+1) \\ s_{L-1}(t+1) \\ \vdots \\ s_3(t+1) \\ s_2(t+1) \\ s_1(t+1) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & c_1 & c_2 & \cdots & c_{L-2} & c_{L-1} \end{pmatrix} \begin{pmatrix} s_L(t) \\ s_{L-1}(t) \\ \vdots \\ s_3(t) \\ s_2(t) \\ s_1(t) \end{pmatrix}$$

と表される。即ち、

【０００８】

【数５】

$$s(t+1) = T_s s(t)$$

である。ここに、T_s は状態遷移行列である。従って、ｉクロック後の線形フィードバックシフトレジスタの状態は、状態遷移行列のべきT_s^iを用いて、

【０００９】

【数６】

$$s(t+i) = T_s^i s(t)$$

のように表される。上記線形フィードバックシフトレジスタの構成には他にモジュラー型、ハイブリッド型が存在する。これらは、Laung-Terng Wang, Edward J. Mccluskey著の論文、"Hybrid Designs Generating Maximum-Length Sequences," IEEE Trans.on Computer-Aided Design, Vol.7, No.1, January, 1988等に示されている。

【００１０】

【発明が解決しようとする課題】しかしながら、従来のノンリニアフィルタジェネレータ（Nonlinear Filter Generator）においては、線形フィードバックシフトレジスタの各レジスタ値が互いに独立ではないため、出力の１、０の等頻度性が保障されておらず乱数特性が悪かっ※

※た。また、擬似乱数発生装置としてコンビネーションジェネレータ（CombinationGenerator ）を用いれば０、１の等頻度性を保障することができる。図７は、上記コンビネーションジェネレータの概略構成図である。図７に示す様に、上記コンビネーションジェネレータは、非線形変換関数回路２９に各線形フィードバックシフトレジスタ３１が接続されている構成となっており、各線形フィードバックシフトレジスタ３１の周期の最大公約数が１である場合にそれぞれの線形フィードバックシフトレジスタ３１の出力系列を独立とみなすことができる。さらに各線形フィードバックシフトレジスタ３１の出力における１、０の等頻度性が保障されるならば、非線形変換関数回路２９への入力はまったくランダムな系列とみなすことができる。１、０の出現頻度が如何に偏った系列であってもランダムな系列とビット毎に排他的論理和演算を施した系列はランダムな系列となる。したがって、上記コンビネーションジェネレータにおいて、１、０が等頻度となるような非線形変換関数回路２９は、少なくとも１つの入力を残りの入力の非線形変換値と排他的論理和演算を施す構成とすればよい。すなわち、非線形変換関数は、

【００１１】

【数７】

$$f(x_1, x_2, \cdots, x_k) = g(x_1, \cdots, x_{i-1}, x_{i+1}, x_k) + x_i \qquad \cdots(2)$$

【００１２】

【課題を解決するための手段】上記目的を達成するため、本発明は、暗号通信装置などで使用される擬似乱数を発生させる擬似乱数発生装置において、クロックに同期して動作するｍ系列を生成する線形フィードバックシフトレジスタと、上記線形フィードバックシフトレジスタの各レジスタ値を非線形変換して１ビットの出力を得る非線形変換関数手段と、上記線形フィードバックシフトレジスタに初期値を設定する初期値設定手段と、上記線形フィードバックシフトレジスタ内少なくとも１つの

とすればよいことになる。ここで、x_i, f, $g \in \{0, 1\}$ である。ところが上記コンビネーションジェネレータを用いたとき暗号の強度を高くしようとするとフィードバックレジスタを多数用意しなければならず、上記ノンリニアフィルタジェネレータに比べてハード構成が大きくなるという欠点があった。本発明は、上記事情に鑑みてなされたものであって、出力の１、０の等頻度性を保障して良好な乱数特性を得ることができる擬似乱数発生装置としてのフィルタジェネレータを提供することを目的とする。

5

線形フィードバックシフトレジスタのレジスタ値を残りの線形フィードバックシフトレジスタのレジスタ値の非線形変換値と排他的論理和演算を施して擬似乱数として出力する排他的論理和演算手段とを具備することを特徴とする。本発明の他の特徴は、暗号通信装置などで使用される擬似乱数を発生させる擬似乱数発生装置において、クロックに同期して動作するｍ系列を生成する線形フィードバックシフトレジスタと、上記線形フィードバックシフトレジスタの各レジスタ値を線形変換し出力する線形変換手段と、上記線形変換値を非線形変換して１ビットを出力する非線形変換手段と、上記線形フィードバックシフトレジスタに初期値を設定する初期値設定手段とを具備し、上記非線形変換手段は、上記線形変換手段の少なくとも１ビットの出力を残りの線形変換手段の非線形変換値と排他的論理和演算を行い擬似乱数として出力するものであって、上記線形変換手段は、線形フィードバックシフトレジスタの状態遷移行列のべきで表現できることである。

【００１３】

【発明の実施の形態】以下、本発明を図示した実施形態に基づいて説明する。図１は、本発明による擬似乱数発生装置としてのノンリニアフィルタジェネレータの一実施形態を示す構成図である。図１に示す様に、このノンリニアフィルタジェネレータは、ｍ系列を生成するＬ段の線形フィードバックシフトレジスタ３３と、上記線形フィードバックシフトレジスタ３３に接続された非線形変換関数回路３５と、上記非線形変換関数回路３５と出力端子３７との間に接続された排他的論理和演算回路３＊

$$f(x_1,\cdots,x_n)=g(x_1,\cdots,x_{m-1},x_{m+1},x_n)\oplus x_m \qquad \cdots(3)$$

と表現できる。ここで、$x_i=s_a$，（$1\leqq i\leqq n$）ただし、$1\leqq a_1<a_2<\cdots<a_n\leqq L$である。また、ｆ，ｇ∈｛０，１｝である。上記線形フィードバックシフトレジスタ３３の１周期においては、非線形関数への入力（x_1，…，x_n）は、（０，…，０）以外の各種を2^{L-n}回ずつ、（０，…，０）を$2^{L-n}-1$回とることがわかる。もし、（x_1，…，x_n）において各種の出現確率が同じであるならば、ノンリニアフィルタジェネレータの出力の１、０の出現確率は等しい。これは、（x_1，…，x_n）において各種の出現確率が同じであるならば、ｇへの入力（x_1，…，x_{m-1}，x_{m+1}，x_n）がある特定値であるとき、x_mは１、０を等頻度でとるからである。しかし、実際は、（x_1，…，x_n）において（０，…，０）をとる場合が他の値をとる場合より１回少ない。従って、ｆ（０，…，０）の値が１回分少なくなる。以上から、$z_0=f(0,\cdots,0)$とすれば、線形フィードバックシフトレジスタの１周期において、出力がz_0となるのは$2^{L-n}-1$回であり、出力が

【数９】

$$z_0\oplus 1$$

となるのは2^{L-n}回である。Ｌが十分に大きければ、上記ノンリニアフィルタジェネレータにおける出力の１、０の出現確率は等しいとみてよいこととなる。次に、上記図１に示したノンリニアフィルタジェネレータの具体例について説明する。図２は、上記図１に示したノンリニアフィルタジェネレータの具体例の構成図である。図２に示す様に、このノンリニアフィルタジェネレータは、線形フィードバックシフトレジスタ４３が、４段のＤ型フリップフロップ４５～５１と、４段目のＤ型フリップフロップ５１の出力と１段目のＤ型フリップフロップ４５の出力との排他的論理和演算を行って上記１段目のＤ型フリップフロップ４５へ出力する第１の排他的論理和回路５３とを有しており、上記各Ｄ型フリップフロップ４５～５１には初期値設定用の入力端子５５およびクロック信号入力用のクロック端子５７が接続されている。そして、このノンリニアフィルタジェネレータの非線形変換関数回路５９が、上記１段目のＤ型フリップフロップ４５に設定されている値と上記４段目のＤ型フリップフロップ５１に設定されている値との論理積演算を

6

＊９とを有しており、上記排他的論理和演算回路３９のもう一方の入力には、上記Ｌ段の線形フィードバックシフトレジスタ３３の少なくとも１段３３ａの出力が接続されている。また、上記Ｌ段の線形フィードバックシフトレジスタ３３には初期値入力のための入力端子４１が接続されている。次に、上記ノンリニアフィルタジェネレータの動作について説明する。

【００１４】上記入力端子４１より初期値が設定されシフト動作する上記Ｌ段の線形フィードバックシフトレジスタ３３の所定の１段のレジスタ３３ａを除くレジスタよりの各レジスタ値が、上記非線形変換関数回路３５へ入力され非線形変換される。そして、上記非線形変換関数回路３５よりの非線形変換値に対し、上記所定の１段のレジスタ３３ａよりのレジスタ値を上記排他的論理和演算回路３９によって排他的論理和演算し擬似乱数系列として上記出力端子３７より出力する。次に、上記構成動作のノンリニアフィルタジェネレータの出力における１、０の等頻度性について説明する。上記Ｌ段の線形フィードバックシフトレジスタ３３の各レジスタ値をs_1，s_2，…，s_Lとし、ｍ系列を発生するものとする。ただし、$s_i\in\{0,1\}$とする。すると、この線形フィードバックシフトレジスタ３３は2^L-1なる周期を持つから、その１周期において（s_1，s_2，…，s_L）≠（０，０，…，０）以外の全ての状態を１回ずつとる。また、非線形関数は、

【００１５】

【数８】

施すための論理積演算回路６１を有しており、上記論理積演算回路６１の出力と上記２段目のＤ型フリップフロップ４７の出力との排他的論理和演算が第２の排他的論理和演算回路６３によって施され出力端子６５より出力される。

【００１６】次に、上記ノンリニアフィルタジェネレータの動作について説明する。まず、上記線形フィードバックシフトレジスタ４３内のＤ型フリップフロップ４５～５１に上記入力端子５５を通して初期値が設定される。上記クロック端子５７よりクロック入力があると、上記Ｄ型フリップフロップ４７～５１にはそれぞれＤ型フリップフロップ４５～４９に記憶されていた値が設定され、上記１段目のＤ型フリップフロップ４５には上記１段目のＤ型フリップフロップ４５に記憶されていた値と上記４段目のＤ型フリップフロップ５１に記憶されていた値の排他的論理和値が設定される。上記非線形変換関数回路５９（論理積演算回路６１）は線形フィードバックシフトレジスタ４３の各レジスタの出力のうち上記１段目のＤ型フリップフロップ４５および４段目のＤ型フリップフロップ５１に設定されている値の論理積値を出力し、上記論理積値と上記２段目のＤ型フリップフロップ４７に設定されている値の排他的論理和演算を施した値が出力端子６５より出力される。従って、初期値として上記Ｄ型フリップフロップ４５～５１の全てに１を設定したとすると、上記出力端子６５に現れる出力系列は、０，１，１，１，０，０，１，０，１，１，０，０，０，１，１の繰り返しとなり、１，０の出現確率は等しいとみてよいことがわかる。

【００１７】次に、上記図２に示した具体例の変形例について図３を参照して説明する。図３に示したノンリニアフィルタジェネレータは、図２に示したものと等価となっている。すなわち、図３に示す様に、このノンリニアフィルタジェネレータは、線形フィードバックシフトレジスタ６７が、４段のＤ型フリップフロップ６９～７５と、４段目のＤ型フリップフロップ７５の出力と１段目のＤ型フリップフロップ６９の出力との排他的論理和演算を行って上記１段目のＤ型フリップフロップ６９へ出力する第１の排他的論理和回路７７とを有しており、上記各Ｄ型フリップフロップ６９～７５には初期値設定用の入力端子７９およびクロック信号入力用のクロック端子８１が接続されている。そして、このノンリニアフィルタジェネレータの非線形変換関数回路８３が、上記１段目のＤ型フリップフロップ６９に設定されている値と上記４段目のＤ型フリップフロップ７５に設定されている値との排他的論理和演算を施す第２の排他的論理和演算回路８５と、上記３段目のＤ型フリップフロップ７３に設定されている値と上記第２の排他的論理和演算回路８５の出力との論理積演算を施すための論理積演算回路８７とを有しており、上記論理積演算回路８７の出力と上記１段目のＤ型フリップフロップ６９の出力との排他的論理和演算が第３の排他的論理和演算回路８９によって施され出力端子９１より出力される。従って、初期値として上記Ｄ型フリップフロップ６９～７５の全てに１を設定したとすると、上記出力端子９１に現れる出力系列は、１，１，１，０，０，１，０，１，１，０，０，０，１，１，０の繰り返しとなり、これは図２に示したノンリニアフィルタジェネレータの出力端子６５に現れる系列が１クロックだけ遅れた系列であるため、同じ系列である。

【００１８】以下に図３に示したノンリニアフィルタジェネレータが図２に示したノンリニアフィルタジェネレータを等価変換することによって作られたものであることを示す。図２において時刻ｔにおける１段目のＤ型フリップフロップ４５のレジスタ値をｓ（ｔ）で表す。すると、２段目のＤ型フリップフロップ４７はｓ（ｔ－１）となり、３段目のＤ型フリップフロップ４９、４段目のＤ型フリップフロップ５１はそれぞれ、ｓ（ｔ－２），ｓ（ｔ－３）と表される。従って、出力端子６５に現れる時刻ｔにおける出力は、

【００１９】

【数１０】

$$s(t)s(t-3)\oplus s(t-1) \qquad \cdots(4)$$

となる。ここで、線形フィードバックシフトレジスタ４３の構造から、

【００２０】

【数１１】

$$s(t)=s(t-1)\oplus s(t-4) \qquad \cdots(5)$$

なる関係が成り立つ。同様に、図３において時刻ｔにおける上記１段目のＤ型フリップフロップ６９のレジスタ値を

【００２１】

【数１２】

$$\bar{s}(t)$$

で表すると、出力端子９１に現れる時刻ｔにおける出力は、

【００２２】

【数１３】

$$(\bar{s}(t)\oplus\bar{s}(t-3))\bar{s}(t-2)\oplus\bar{s}(t) \qquad \cdots(6)$$

となり、上記線形フィードバックシフトレジスタ６７の構造から、

【００２３】

【数１４】

$$\bar{s}(t)=\bar{s}(t-1)\oplus\bar{s}(t-4) \qquad \cdots(7)$$

が成り立つ。上記出力端子９１に現れる出力が上記出力端子６５に現れる出力に対して１クロック遅れているから、ｓ（ｔ）と

【００２４】
【数１５】

$$\bar{s}(t)$$

の間には、
【００２５】
【数１６】

$$\bar{s}(t) = s(t-1)$$

なる関係がある。これを上記式（６）に代入すれば、
【００２６】
【数１７】

$$(s(t-1) \oplus s(t-4))s(t-3) \oplus s(t-1) \quad \cdots(8)$$

を得る。また、上記式（７）の関係と
【００２７】
【数１８】

$$\bar{s}(t) = s(t-1)$$

を組み合わせて上記（８）式に代入すれば、上記（４）式を得ることができる。従って、上記図３のノンリニアフィルタジェネレータが図２のノンリニアフィルタジェネレータを等価変換することによって作られたものであることがわかる。上記の変形実施例を含めて本発明を一般化して表現すると図8 のようになる。同図において、図1 と同じ構成には同じ符号を付した。図8 が図1 と異なる点は、線形フィードバックシフトレジスタ３３と非線形変換回路３５との間に、線形フィードバックシフトレジスタ３３の状態遷移行列T_sのべきT_s^{ℓ}で表される線形変換回路１００を配置したところにある。先に述べたように図８における線形フィードバックシフトレジスタ３３の状態遷移行列T_sのべきT_s^{ℓ}で表される線形変換回路１００の出力は、線形フィードバックシフトレジスタ３３の状態出力をｉクロック分時間シフトしたものであるから、図１に示されるノンリニアフィルタジェネレータと同様に、図８に示されるノンリニアフィルタジェネレータの出力における１，０の出現確率も等しいとみてよいこととなる。例えば、図３の構成を図８に基づいて表現すると図９のようになる。同図において１０１が線形変換回路である。このときの線形フィードバックシフトレジスタ６７の状態遷移行列T_sは、
【００２８】
【数１９】

$$T_s = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

であり、線形変換回路１０１はT_sのべきとなる。この例では$T_s^{\ell} = T_s$となる。線形フィードバックシフトレジスタ６７の状態を、
【００２９】
【数２０】

$$s(t) = (s_4(t), s_3(t), s_2(t), s_1(t))^T$$

と表し、線形変換回路１０１の出力を
【００３０】
【数２１】

$$u(t) = (u_4(t), u_3(t), u_2(t), u_1(t))^T$$

と表せば、
【００３１】
【数２２】

$$u(t) = T_s s(t)$$

すなわち、
【００３２】
【数２３】

$$\begin{pmatrix} u_4(t) \\ u_3(t) \\ u_2(t) \\ u_1(t) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} s_4(t) \\ s_3(t) \\ s_2(t) \\ s_1(t) \end{pmatrix}$$

と表せるので、これより、
【００３３】
【数２４】

$$u_1(t) = s_1(t) \oplus s_4(t),$$

$$u_2(t) = s_1(t),$$

$$u_3(t) = s_2(t),$$

$$u_4(t) = s_3(t)$$

を得る。従って、図３の場合は線形変換回路が図９のように表されることになる。
【００３４】
【発明の効果】本発明は、以上説明したように、クロック入力に同期して動作する線形フィードバックシフトレジスタの各レジスタ値を非線形変換関数回路に入力し、クロック毎に擬似乱数を出力する構成において上記線形フィードバックシフトレジスタの少なくとも１つのレジスタ値を残りのいくつかのレジスタの非線形変換値と排他的論理和演算を施す様にしているので、或いは、線形フィードバックシフトレジスタの各レジスタ値を線形変換回路に入力し、その出力である線形変換値を非線形変換回路に入力したものにあっては、線形変換出力の少なくとも１ビットの出力を残りのいくつかの線形変換出力の非線形変換値と排他的論理和演算を施すようにしてい

るので、１，０の出現が等頻度である乱数特性のよい擬似乱数発生装置が提供できる。

【図面の簡単な説明】

【図１】本発明による擬似乱数発生装置としてのノンリニアフィルタジェネレータの一実施形態を示す構成図である。

【図２】上記図１に示したノンリニアフィルタジェネレータの具体例の構成図である。

【図３】図２に示したノンリニアフィルタジェネレータの変形例の構成図である。

【図４】一般のストリーム暗号装置の構成図である。

【図５】従来の擬似乱数発生装置の一例であるノンリニアフィルタジェネレータの構成図である。

【図６】一般のスタンダード型の線形フィードバックシフトレジスタの構成図である。

【図７】従来の擬似乱数発生装置の一例であるコンビネ＊ーションジェネレータの構成図である。

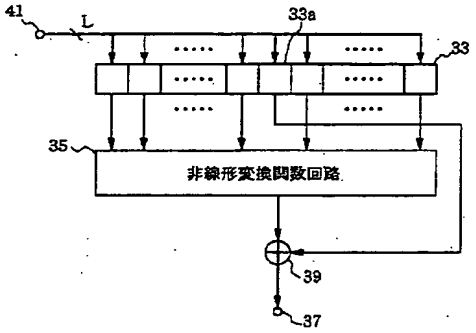
【図８】本発明に係る説明図である。

【図９】本発明に係る説明図である。

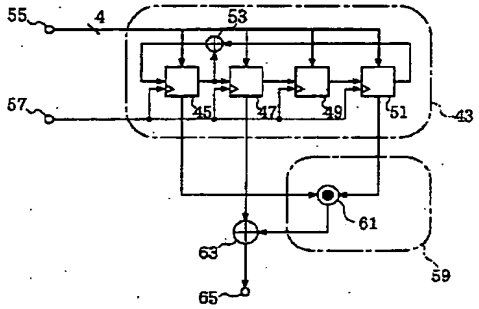
【符号の説明】

１…平文入力端子、　３…暗号文出力端子、５、３９、５３、６３、７７、８５、８９…排他的論理和演算回路、７…擬似乱数発生装置、９、１３、４１、５５、７９…初期値設定用端子、１１、１５、５７、８１…クロック入力用端子、１７、３３、４３、６７…線形フィードバックシフトレジスタ、１９、２９、３５、５９、８３…非線形変換関数回路、２１、３７、６５、９１…擬似乱数出力端子、２３、４５～５１、６９～７５…Ｄ－ＦｌｉｐＦｌｏｐ素子、２５…排他的論理和演算素子、３１…線形フィードバックシフトレジスタ、６１、８７…論理積演算回路、

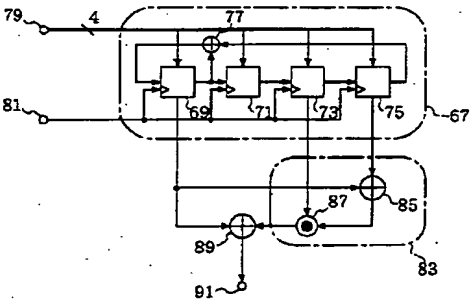
【図１】



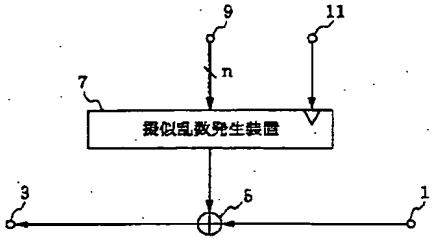
【図２】



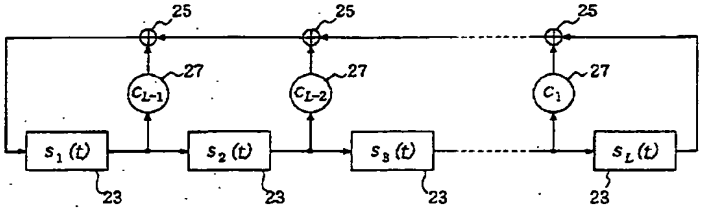
【図３】



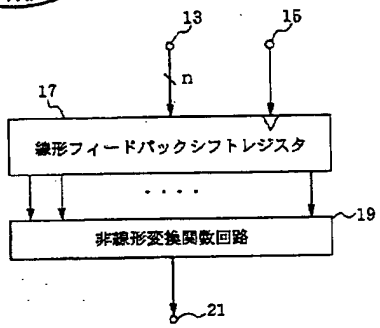
【図４】



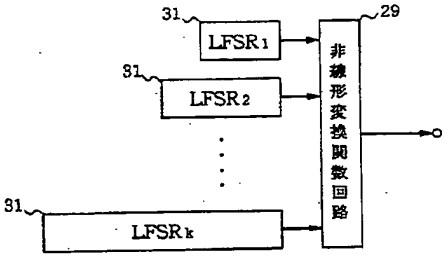
【図６】



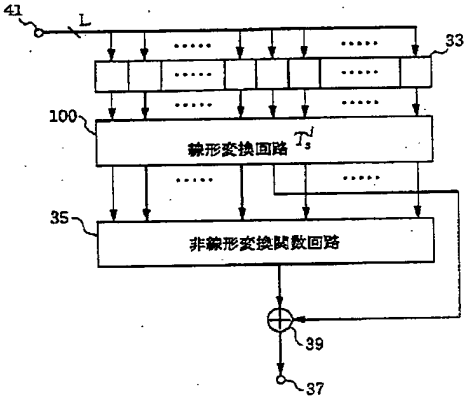
【図５】



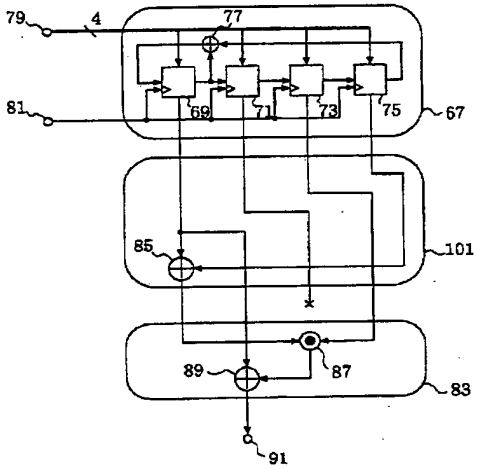
【図７】



【図８】



【図９】



フロントページの続き

(72)発明者　杉本　浩一
神奈川県高座郡寒川町小谷二丁目１番１号
東洋通信機株式会社内